MITRE TECHNICAL REPORT

State of the Art Biometrics Excellence Roadmap

Certified Products List (CPL) Expansion: The Way Ahead

October 2008, v. 1.2

Margaret Lepley
Joseph Marques
Norman Nill
Nicholas Orlans
Rod Rivers
Ron White

Sponsor:	Scott Swann, Program Manager	**Contract No.:**	J-FBI-07-164
Dept. No.:	G122	**Project No.:**	14008FC09-LA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This document was originally published June 2008, and reflects the state-or-the-art as of that date.

MITRE

Executive Summary

The FBI has extensive experience in fingerprint product certification. The introduction of the Next Generation Identification (NGI) system with its integrated, multi-biometric focus increases the need for product certification services. As additional biometric modalities are added, the FBI will be called upon to certify an ever increasing number of products. Partners and other stakeholders around the world will continue to look to the FBI for product certification leadership in this growing and increasingly critical area.

Broader FBI adoption of emerging biometrics requires acknowledging a prevailing commercial focus. The performance of non-contact modalities (non-fingerprint sensors) is susceptible to environmental and operational scenarios. Specifically, certification must consider device standards, environmental factors, collection guidelines, and feedback mechanisms to ensure that identification services are both enabled and sustained. Certification compliance must therefore strive to become lifecycle based, rather than act as a gatekeeper.

Face recognition is probably the next non-contact modality to be implemented within NGI; however, the rapid development of digital cameras used for facial recognition throughout government and industry makes it impractical to propose a device certification process similar to fingerprint. Consumer cameras, made inexpensive by economies-of-scale, already exceed reasonable facial performance criteria. Requests for certification would not only overwhelm the process, but quickly become obsolete as new models are continuously replaced. In contrast, the currently smaller Iris camera market better lends itself to a device certification program.

Our findings indicate that the FBI can achieve the greatest benefit by adopting a certification program process that leverages existing domestic standards efforts, formalizes biometric best practices and helps participating agencies test and sustain compliance. Studies have shown that many biometrics do provide accuracy and interoperability when properly implemented, but that deficiencies go unnoticed and remain without feedback. Booking site operators also require sensible, operational guidance.

Provide Compliance Services

Post-deployment identification accuracy is more difficult to maintain for non-contact biometrics because environmental issues have a greater influence. Continuous monitoring and feedback is integral to ensuring that devices operate at peak efficiency, operators follow best-practice guidance, and configuration changes are detected. We recommend that the FBI pursue quality monitoring services to sites and partners as follows:

- Develop open image-quality metrics for iris and face imagery assessment.
- Provide operationally relevant feedback to sites based on observations of biometric quality or other attributes.
- Generate CJIS reports describing the quantity, quality, and attributes of biometric submissions by state and agency.

- Encourage submission improvement over time based on measurable criteria.
- Enable early detection and correction of emerging quality issues (e.g., hardware production differences) before substantial data is gathered.
- Provide a way for sites to submit test enrollments for conformance testing, deployment, and training.

Promote and Extend ANSI/NIST Standards with Criminal Justice Focus

Historically, the FBI has promoted interoperability through American National Standards Institute (ANSI)/National Institute of Standards and Technology (NIST)-ITL 1-2007. The introduction of International Standards Organization (ISO) (19794-x) biometric standards has complicated matters. Despite many similarities, the ISO standards are not always an ideal vector for criminal justice and forensic applications. In order to sustain a long-term operational focus on criminal justice needs, the FBI should promote and extend the ANSI/NIST standards whenever possible to include certification processes, guidelines, and other practice recommendations. Distinct or conflicting needs should be harmonized with the ISO specification, but not be subject to its commercial interests.

The FBI should continue to promote the ANSI/NIST standard since law enforcement agencies participated in its development and voted on its approval. Areas of specific reinforcement include:

- Review and adapt normative requirements for other biometric modalities to provide compatibility but permit criminal justice extensions
- Baseline the acquisition behavior of proprietary systems (e.g., iris) and create subject acquisition profiles for both historic and future collection standards
- Reflect the emerging biometric needs of forensic examiners and analysts.

Distill, Formalize, and Promote Best Practices for Image Acquisition

Investigations such as the FBI/Bureau of Prisons (BOP) Benchmark Study show that, despite the availability of informative standards guidance, image capture quality varies considerably. Environment, process, lighting, and camera differences negatively affect identification performance. The best practice guidance of ANSI/NIST and ISO standards exhibit a reasonable set of requirements and already have good stakeholder support. Given these precedents, it would be ineffective to introduce a new set of requirements.

In conjunction with continued promotion of ANSI/NIST standards, we recommend that the FBI expand upon the best practices provided in ANSI/NIST Annexes H & I and ISO/IEC 19794-5 Annex B. Recommendations for refinement include:

- Develop concise booking environment recommendations and guidance suitable for diverse agency partners and experience levels.

- Provide model procurement specifications for mugshot systems and capture environments to create an common baseline.
- Require the minimal adoption of Subject Acquisition Profile 40 and encourage continued progress toward profiles 50/51.
- Develop and integrate real-time quality assessment tools that provide operators with instantaneous feedback to help ensure conformance during enrollment.
- Initiate the development of iris Subject Acquisition Profiles consistent with the needs of the criminal justice community and link to device requirements.

Acknowledgements

This report was actively supported by many dedicated individuals and experts within the FBI and the National Institute of Standards and Technology (NIST). The authors wish to acknowledge special thanks to Tom Hopper, Dr. Hiro Nakosone, Richard Vorder Bruegge, and Dr. Nicole Spaun. We also thank Dr. John Butler of NIST for his review and comments.

Table of Contents

List of Figures

List of Tables

1 Roadmap

Currently the FBI certification program is centered on the performance of fingerprint sensors. Even within this modality, pressures have emerged based on the development of ultrasonic and contactless sensor designs. Hardware lifecycles, manufacturing concerns, and cost pressures continuously push fingerprint devices in directions that enhance the verification process at the expense of some of the forensic functions that are so critical to the law enforcement community. The challenge for the expansion of the Certified Products List (CPL) has been to adapt to emerging technologies without adversely impacting existing critical FBI identification services.

As the FBI moves to meet the evolving requirement to certify facial and iris devices, it is likely to encounter some political and organizational resistance to change. Stakeholders with a longer history using a particular biometric have built an operational investment in certain use cases, technologies, and data sets. The benefits of this legacy are clear and include organic experience dealing with the capture of the biometric, resolution of interoperability issues during storage and transmission, and ways to improve quality under normal operating conditions. But conversely, new standardization efforts, partnerships, and data sharing efforts can create perceived short-term risks as biometric requirements seem to widen. The introduction of new criminal justice requirements helps biometric performance in the long term, but its adoption must be gradual and cooperative.

Increasing reliance on biometric identification creates challenges to the state and local agencies that provide data and conduct searches. Greater accuracy is needed for both algorithms and analysts as databases grow in size. This puts pressure on personnel who collect biometric samples since it demands higher expectations of quality and introduces newer sensors and technologies. Studies have shown that data quality is often the root cause of match difficulty. Operational guidance is often inadequate and data quality reporting is lacking or not timely.

Several initiatives are necessary to help mitigate these difficulties and pave the way for broader biometric standardization efforts. All rely on partnership with other government agencies, standardization bodies, and biometric vendors that have distinct interests and prior experience that can be leveraged. The challenges of device and process certification are more political than technological. Many of the core ideas and guidance already exist at some level of maturity and it is impractical to reinvent them. Next steps in this process should include:

- Begin to establish quality monitoring services and provide feedback to participating agencies and stakeholders. Biometric data providers will become increasingly reliant on analysis services to ensure that devices are operating correctly and that operators are using them properly. Sites should have a mechanism to submit test enrollments to ensure compliance and complement operational guidance or other best-practice instructions.
- Concise operational guidance on facial image acquisition should be collected and aggregated based on current standards efforts. This effort should include informative guidance on facial image requirements and how to properly set up the capture

environment. The document can be based on current ANSI/NIST efforts and be harmonized with newer standards such as ISO 19794-5 Amendment 1 (Conditions for taking photographs for face image data). The primary goal is to extend existing recommendations but maintain a criminal justice focus that can be guided by FBI requirements instead of broader commercial interests. The document should be submitted for Advisory Policy Board (APB) approval.

- The maturity level of iris recognition systems must be assessed and baselined to determine how criminal justice needs differ from current commercial requirements. This work includes the development of vendor-neutral quality metrics to improve the acquisition process and improve feedback to operational users. Standardization criteria should be developed and extended to include system parameters not currently addressed by current INCITS and ISO standards (e.g., wavelength choice, illumination strength.). This quality metrics document should leverage current works and be harmonized to them, but include expertise from other agencies and vendors to address the anticipated needs of both software and human examiners. Submission to APB for approval should follow.

2 Background

This document provides an overview of the issues and recommendations for the CPL Expansion task for the State of the Art Biometrics Excellence Roadmap (SABER) study. The current certification process works well and is respected by industry and other U.S. Government (USG) agencies, as well as other countries. However new requirements for certification services and technical advances in biometric technologies are forcing the FBI certification process to evolve and assume a leadership role for other classes of biometric hardware.

> "Currently, the FBI's CPL provides minimal specifications for fingerprint capture devices required for interfacing with the FBI's IAFIS. Going forward, this guidance must expand to certification processes for suitable capture equipment of other biometric modalities to interface with the FBI's NGI System. This study shall include detailed recommendations for CPL expansion."[1]

Face and iris recognition may be next in line as mature biometric modes requiring a certification path, but the criteria used for them should be universally leveraged for all modes. Despite differences in sensor design and subject interaction, this document seeks to enumerate many of the issues likely to arise for any biometric. The preliminary assessments of face and iris provide insight into the backgrounds, issues, and lifecycle maturity for each biometric. They provide a

[1] Statement of Work, Federal Bureau of Investigation, State-of-the-Art Biometric Excellence Roadmap (SABER) Study, April 11, 2007.

technology discussion on the unique aspects of those modes, but must be taken in the context of overall certification goals.

2.1 Overriding Motivation

The FBI seeks to establish a preeminent role in biometric infrastructure leadership across a diverse set of partners and stakeholders including local, state, federal, and international organizations. The principal objective is to ensure that biometric query and enrollment services provide acceptable levels of accuracy and interoperability using quality data from a multitude of sources. Key to this goal is the identification of standards and conformance criteria that must be met or exceeded by any participating collection system. The establishment of image quality metrics and procedures that empower local, state, and federal agencies to effectively monitor their biometric capture systems is equally important. These are necessary to identify nascent performance gaps, adapt to emerging sensor designs, maintain data quality from partners, and track improvement over time.

The formalization of standards, certifications, and quality monitoring should serve as a model to other stakeholders, either for direct adoption or as a baseline template for their own efforts. The current maturity of some biometric modalities, such as face and iris and the existence of operational systems, demands a pragmatic approach to biometric quality improvement. Selected criteria must provide benefits consistent with costs, and acknowledge the diverse needs of established data repositories and difficult operational scenarios.

3 Preliminary Assessment of Facial Imaging

The quality of facial images is in large part determined by lighting, camera settings, other environmental factors, and by the level of cooperation of the subject. Most new consumer cameras provide the best value and are more than capable of meeting the facial recognition imaging requirements associated with booking stations. Certification of consumer cameras is not practical and would not significantly affect facial image quality assuming that they already meet Annex I level 40 requirements (See Appendix C for a discussion of ANSI/NIST-ITL 1-2007 Sections 15, Annex H and Annex I**)**

.

The procedures described below focus on building stakeholder support for improving the end-to-end facial image capture process.

Facial identification and verification pose particular challenges to device certification beyond those encountered with fingerprint processes. As a minimal biometric baseline, facial capture process must allow the capture of sufficient quality imagery for:

- The automatic and reliable detection of registration features (e.g., eyes) to normalize images and bootstrap recognition algorithms
- Broad subject classification/estimation of age, gender, race.
- Distinction of real and artificial features (e.g. cosmetics)

- Possible identification or rejection by a human examiner
- Reliability and accuracy of large scale automated search.

Facial matching processes depend on high fidelity imagery in order to minimize the occurrence of false matches and false non-matches. Unlike fingerprint, facial recognition is not a multi-instance biometric mode; consistency and quality become even more important with a single matchable case. The identification process, whether conducted by a human examiner or a software algorithm, will often hinge on the viability of single images.

We must also recognize other difficulties that are relevant to facial imaging sensors (i.e., cameras), but that have reduced applicability in other biometric modes. As a public biometric, face image capture is subject to greater influence from external factors such as subject behavior and environmental conditions. Failure to acknowledge this could result in over-specifying image capture criteria at the expense of other factors (e.g., pose, illumination,) that have greater effects on identification accuracy or forensic analysis.

Therefore, the capture requirements for face imagers must be broadened to include aspects of the capture process in addition to basic measures of fidelity and quality. Fortunately, many of these issues have been addressed by various standards initiatives over the years. Biometrics standards lay out many of the procedural requirements necessary to acquire and store usable facial imagery for human or automated analysis. Imaging standards lay out the criteria necessary to ensure that the sensor (camera) is properly calibrated for color rendition, spatial accuracy, resolution, and other tolerances. The challenge for certification will be to isolate relevant imaging standards, identify human-factors gaps to a repeatable process, qualify operational scenario assumptions, and link it all together to satisfy both biometric standards and the unique requirements of FBI analysts. It will not be enough for a face camera to merely *permit* the acquisition of a quality image. It must actively *facilitate* that acquisition given an appreciation of real world constraints.

3.1 Certification Considerations

Electronic Fingerprint Transmission Specification (EFTS), now Electronic Fingerprint Biometric Specification, or EBTS, Appendix F specifications were largely constrained to aspects of image quality as measured in a normal operating mode. However, facial imaging performance cannot be fully decoupled from the environmental conditions in any given scenario because:

- Face imaging is not a contact biometric; lighting, distance, backgrounds, and subject behaviors are integral to the acquisition
- Both operator and subject are essential to the process
- The imaging sensor is likely based on a generic camera design with applications and functionality that *surpass mere face image collection.*

Therefore, any recommendations for face image capture must take into account more than just the intrinsic aspects of the sensor itself. Extrinsic criteria, describing how the device interacts with its environment and how it accommodates operational variation are equally as important to success.

In order to recommend a device for broad deployment, it will be necessary to qualify the limitations under which it is expected to operate. To do otherwise is to risk collecting data that does not meet quality guidelines for ingestion by FBI systems. In general, many of these factors can be mitigated externally (e.g. lighting, housing), but the basic constraints must still be known, since they bound the conditions under which certification is meaningful.

Environmental

1. What is the operational range of illumination necessary for the camera's optics?
2. What are the spectral characteristics for which white balancing is meaningful?
3. What are the operational tolerances for temperature and humidity?

Behavioral / Installation

1. How must the sensor be installed to ensure proper operation?
2. What steps must an operator perform for correct imaging?
3. What supporting equipment is required to achieve a nominal sensor configuration?

Calibration

1. What steps are required for sensor calibration? Under what conditions should calibration be performed (e.g., time intervals and shock events)?
2. What is the lifespan of a calibration?
3. What settings, options, and configurables must be maintained on the sensor/camera for certified operation?
4. How often should the calibration be validated, and who should do it?

The issues above highlight the need to create certification criteria that address the environmental variation normally encountered to satisfy image exchange standards. Basic requirements for camera resolution and color accuracy, may be the easiest to meet. The selection of criteria needed to achieve these behaviors under real-world operational constraints will be more challenging. Mapping these criteria back to mainstream standards and best practices provides greater justification for their inclusion.

3.2 Facial Feature Levels

Facial imaging terminology lacks some of the finer distinctions commonly used in more established domains such as fingerprint recognition. This has made it more difficult to qualify the level of detail required for particular purposes such as verification, identification, or forensic confirmation. Nevertheless, it is possible to propose feature level classifications that are consistent with those commonly used for fingerprint analysis.

Table 3-1. Suggested Feature Level Details for Face

Classification	Fingerprint Meaning	Face Equivalent
Level 1 features	Large scale patterns in the ridge flow of the print. Detection of core and delta regions and Henry-style classification. Require <500 DPI	Low frequency patterns and arrangement in overall face structure caused by skeletal formation and coarse shape and location of the eyes, nose, and mouth. Require: ~50 interocular pixels
Level 2 features	More granular features of ridge structure including bifurcations and terminations (i.e.. minutiae) along with the presence of scars, creases, or incipient ridges. Require: 500 DPI	Finer details of face features described by predefined and segment-able regions (e.g., eyes, nose, mouth, cheeks) along with creases and larger landmarks such as wrinkles and moles. Require: 90 interocular pixels
Level 3 features	Detailed examination of ridge structure including the presence of pores and variations in shape or width. Require: 1000 DPI	Detailed analysis of skin texture and small, random features including pores, hair follicles, skin tags, and other fine dermatological structures. Require: 120+ interocular pixels

To our knowledge, no definitions have yet been proposed for facial level details, but these should provide a good starting point for discussion and reference. Current requirements for face are given in resolution terms only as an estimated inter-ocular distance in pixels. This should be expanded to include other factors necessary to resolve the finer levels of detail and to provide operational headroom for environmental variation.

3.3 Relevant Biometrics Standards

Guidance on the acquisition, transfer, and storage of face image data is provided by three primary standards. These documents share many attributes in common, reflecting joint development or close references.

- ANSI/NIST-ITL 1-2007: "American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information (Annex I) "
- ISO/IEC 19794-5-2005: "Information technology – Biometric data interchange formats – Face image data"
- ISO/IEC 19794-5:2005/Amendment 1:2007(E) "Conditions for taking photographs for face image data"

ANSI/NIST-ITL 1-2007: "American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information" was approved in April

2007. Section 15 of the document provides packaging guidance for face transmissions in the form of a Type-10 image. A more detailed analysis of ANSI/NIST-ITL 1-2007 is provided in Appendix C "Face Recognition Guidance."

ISO/IEC 19794-5-2005: "Information technology – Biometric data interchange formats – Face image data" was ratified in June 2005. The standard seeks to address four typical application areas:

- Human examination using sufficient resolution to ascertain small features needed for identity verification.
- Human verification of identity by comparison of facial images.
- Computer automated identification using 1-to-many searching.
- Computer automated verification using 1-to-1 matching.

ISO/IEC 19794-5:2005/Amendment 1:2007(E): "Conditions for taking photographs for face image data" was ratified in December 2007. It provides guidance for the design of photographic studios and photo booths.

3.4 Market Considerations

Unlike fingerprint sensors, the digital imaging market is both mature and profitable independent of any biometric concerns. This poses a challenge for certification for a variety of reasons:

- Cameras and other imaging products are released and/or updated on a much more aggressive schedule than any traditional biometric device. Prolonged certification may only reflect obsolete products at completion.
- Camera designs typically serve a variety of use cases. Designs that pass certification may contain numerous undesirable features that are incompatible with consistent and reliable image capture (e.g., switches, options, and settings that should never be used in practice).
- Product designs may change without warning even within a single model line. There is no guarantee that a manufacturing process will be invariant over the lifetime of a product. Component substitution, manufacturing variation, and software/firmware upgrades may be unavoidable in practice.

It would be ineffective for the FBI to certify specific cameras at this time. Instead, a collection system would be required to meet specific guidelines. Documents providing collection recommendations to aid in meeting those guidelines will be generated. Imagery submitted to the FBI from a collection system will be rated by the FBI, to provide feedback to the collection system on how well the system is meeting the guidelines.

3.5 Conclusion

- Facial recognition technology provides accuracy and interoperability if quality imagery is obtained.

- Image quality is dependent on the overall capture system given a process, environment, lighting, camera settings, and control.
- It is impractical to certify consumer cameras because there would be too many certification requests. Consumer cameras meeting Subject Acquisition Profile (SAP) level 40 would not benefit from certification since device performance is not the main problem. Instead, standardization of enviornment, process, and claibration are key.
- The FBI should continue to use and expand on ANSI/NIST Annex I Best Practice Recommendations for facial image acquisition since it has a reasonable set of requirements and good stakeholder support. It would be difficult and ineffective to introduce a totally new set of requirements.
- Many existing mugshot systems within criminal justice were not implemented to current facial recognition requirements. See the FBI/Bureau of Prisons (BOP) benchmark study, dated 22 Jaunary 2008.

3.6 Recommendations

- Promote ANSI/NIST Annex I and harmonize with ISO standards.
- Develop FBI recommendations that are based on and reference Annex I, but provide the information with a focus on the booking environment.
- Provide model procurement text for mugshot systems.
- Develop open image quality metrics that agencies can use in their systems.
- Generate CJIS reports showing quantity and quality of submissions by state and agency.
- Identify face features necessary to facilitate human identification tasks and map these back to objective resolution/quality metrics needed in the capture process.

4 Preliminary Assessment of Iris Recognition

Iris recognition represents a distinct challenge for certification because the dominant providers of the technology all rely on patented, intellectual property from a single vendor. In 1987, the U.S. Patent and Trademark Office granted a concept patent on iris identification based on the work of two ophthalmologists, (L. Flom and A. Safir, U.S. Patent No. 4641349 (1986), International patent WO8605018A1 (1986)). This was followed up in 1994 when Dr. John Daugman was awarded a patent on a specific, automated algorithm for recognizing the iris. Shortly thereafter, the technology was successfully commercialized by Iridian Technologies through partnerships with several device integrators. L1 Identity Solutions Inc. assumed patent rights to the Daugman algorithm with the acquisition of Iridian Technologies in 2006.

The concept patent expired in 2005, thus opening the doors to other implementations, but the traces of a single, dominant implementation persist in the systems, databases, and standards used today. Until recently, competition was limited to the integrators who licensed technology from

Iridian. With protection afforded by the concept patent and interoperability assured by the Daugman patent, systems were broadly deployed without the competition and testing more common in face and fingerprint biometrics.

The certification process must contend with this entrenched capability and deconstruct many development decisions to promote accuracy and interoperability among both old and emerging stakeholders.

Currently there is very limited deployment of iris recognition systems within criminal justice. Moving the industry toward improved interoperability will likely require a unified effort across several federal stakeholders.

4.1 Certification Considerations

Iris recognition shares many of the same issues as facial image capture since it, too, is a non-contact biometric requiring an image sensor. But the acquisition process is more constrained and has less environmental sensitivity since it provides its own integrated illumination. Nevertheless, high quality, repeatable iris capture is not a task that operators and subjects are intuitively prepared to perform. Certification must consider human factors issues perhaps at least as seriously as engineering quality metrics.

The certification process is exacerbated by several years of pre-existing sensors and data sets. It is reasonable to assume that partners and stakeholders will need to continue using this data long after certification guidelines are implemented and adopted. Substantial deviations from established practice may degrade interoperability efforts and data sharing.

4.1.1 Wavelength Choice

Iris imaging has historically presumed an illumination source operating in the near infrared wavelengths between 700 and 900 nanometers. This range was chosen for two reasons; it is non-intrusive (invisible) to the subject and it is better at revealing the structure in darkly pigmented irises. There is no established consensus regarding the precise wavelength that is best or, indeed, if only a single wavelength should be used. Variations in iris pigmentation among differing ethnic populations further complicate any optimal selection. Standards have remained intentionally vague in this regard and refer to the band in terms of "current best practice," but do not preclude other choices, even the visible spectrum.

Variations in wavelength due to either sensor design or ambient environmental illumination do affect match score performance.[2] The impact level is likely a function of the spectral overlap between any two imaged irises. The choice of illumination wavelength may vary among commercial implementations.

[2] C. Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li, " Multispectral Iris Analysis: A Preliminary Study," Proc. of IEEE Computer Society Workshop on Biometrics. New York, June 2006.

4.1.2 Dual Eye vs. Single Eye Acquisition

Sensors can be designed to capture iris images individually or jointly. Single eye systems benefit from simplicity and lower cost thanks to reduced optics, sensors, and computational needs. But individual scanning implies a sequential activity that increases enrollment time and risks left-right mis-assignment. Dual eye systems are more complex because a larger space must be imaged, processed, and segmented to isolate each iris. Enrollment throughput can be faster, with less risk of left-right iris swapping, but some flexibility in obtaining individualized, best-quality iris images is lost.

The use of slaps during fingerprint enrollment as a means to ensure proper finger sequencing may serve as a precedent in selecting dual-eye imagers. Mobile sensors may continue to image a single eye due to cost and size constraints. It may be possible to confirm the expected location of tear ducts for left and right scans, which would identify sequencing errors.

4.1.3 Simultaneous Face and Iris Capture

Combined face and iris acquisition is desirable to help guarantee an integrated identity record and speed enrollment times. Prototype systems such as Honeywell's CFAIRS (Combined Face and Iris System) are still in the early stages of development and refinement.[3] From a certification standpoint, the emergence of integrated systems complicates quality decisions. The final accept or reject decision must be based on a combination of individual assessments, no one of which can be optimized.

4.1.4 Integrated Quality Determination Criteria

Iris capture devices have an integrated quality assessment function that keeps poorly positioned, obscured, or blurry images from being used for recognition. These mechanisms are not always effective and the manufacturer can adjust the decision policy. Many ideas have been proposed for iris quality, but there is no universal quality metric in the industry. Proprietary techniques utilize some combination of various attributes including, but not limited to:

- Iris size (pixels)
- Pupil dilation/contraction (pixels)
- Image contrast
- Iris texture
- Occlusion (due to eyelid closing or specular reflections)
- Focus and blur measures
- Off-axis gaze

[3] Honeywell patent: http://www.wipo.int/pctdb/en/wo.jsp?wo=2007103833&IA=WO2007103833

Integrated quality assessment is key to fast and accurate iris acquisition without requiring an operator to subjectively inspect imagery. Current implementations seem to enforce a superset of the criteria enumerated in iris standards documents. Significant differences in interpretation or thresholds risk creating performance gaps for some sensor/algorithm combinations.

4.1.5 Illumination Exposure and Eye Safety Considerations

Iris recognition systems use active illumination in the near infrared wavelengths to better resolve the details of iris structure in the image. Even if the ambient environment provides sufficient illumination in this band, it is unlikely to be consistent, and unwanted reflections may obscure the iris itself. For reliable capture, the camera must be integrated with illuminators (typically LEDs) using the right wavelength(s), angles, and power.

The eye responds to light in the visible range (380 to 750 nanometers.[4]) The pupil will not dilate or contract in response to light in the near infrared wavelengths (750 to 1400 nm) since these are not perceived. Pupil contraction serves a vital function by minimizing the amount of light reaching the retina when the environment supplies a hazardous amount of energy. It is conceivable that a subject can gaze into an infrared illuminator for a prolonged time or at a close distance without any aversion response. Any system utilizing an infrared illumination source needs to consider this issue.

For most commercial iris recognition systems, hazard issues are insignificant since the amount of energy is small and the duty cycle of the sensor is limited. But some prototype systems such as Sarnoff's Iris on the Move and Honeywell's CFAIRS perform iris scanning at a distance. They require larger illumination sources and must address safety issues more thoroughly since there can be secondary effects on bystanders (e.g., operators, security guards.).

As the FBI moves forward with iris device certification, eye safety issues should be addressed with the help of the standards referenced below. Public perception of eye safety could be negatively affected by prototype systems even in the absence of risk. FBI coordination with ANSI, the Underwriters Laboratory (UL), and other organizations may be beneficial.

There is a large body of work that addresses eye hazards and illumination limits. A selected list is provided below:

4.1.6 References

Documentation of the Threshold Limit Values for Physical Agents, ACGIH Worldewide, 2001.

Recommended Practice for Photobiological Safety for Lamps and Lamp Systems–General Requirements, ANSI-IESNA, RP-27.1-05, 2005.

[4] Source: Wikipedia: Visible Spectrum, http://en.wikipedia.org/Visible_spectrum.

Recommended Practice for Photobiological Safety for Lamps and Lamp Systems–Measurement Techniques, ANSI-IESNA, RP-27.2-00, 2001.

Recommended Practice for Photobiological Safety for Lamps and Lamp Systems–Risk Group Classification & Labeling, ANSI-IESNA, RP-27.3-96, 1996.

American National Standard for Safe Use of Lasers, Laser Institute of America, ANSI Z136.1–2007, 2007.

Measurements of Optical Radiation Hazards, R. Matthes and D. Sliney (editors), ICNIRP and CIE, 1998.

International Standard, Photobiological safety of lamps and lamp systems, International Electrotechnical Commission, IEC 62471/CIE S-009:2002, 2006.

OSHA Technical Manual, U.S. Department of Labor, http://www.osha.gov/dts/osta/otm/otm_iii/otm_iii_6.html.

Ocular hazards of light, D. Sliney, International Lighting in Controlled Environments Workshop, T.W. Tibbitts (editor), 1994.

Biohazards of ultraviolet, visible, and infrared radiation, D. Sliney, Journal of Occupational Medicine , Vol. 25, 203-2006, 1983.

Interaction of laser radiation with structures of the eye, R. Mihran, IEEE Transactions on Education (1991), Vol. 34, 250-259. IEEE Symposium on Product Safety Engineering, IEEE, 1-5, 2005.

Evaluation of optical radiation hazards, D. Sliney and B. Freasier, Applied Optics, Vol. 12, 1-24, 1973.

4.2 Iris Feature Levels

Thus far, iris recognition techniques have not relied on isolated features within the iris structure for the purposes of pattern matching. Detection of the pupil, sclera, and eyelid boundaries is required for segmentation, but the analysis of the iris region itself is done in a global pattern matching space. Moreover, the use of near infrared illumination helps to reveal iris texture, but the loss of visible wavelengths does little to assist the human examiner who is accustomed to common eye color classifications.

Table 4-1 provides feature level classifications in the spirit of those used for fingerprint analysis. In keeping with the ISO iris standard, Level 1 begins at a "low" level of image quality (100 pixel diameter). At these resolutions, automated analysis and matching is viable, but the determination of unique features by a human examiner is unlikely to be repeatable or complete, especially for many dark-eyed subjects. The Level 2 classification starts to provide an examiner with enough detail to describe the prominent features common to iris structure and referenced in ophthalmic literature. However, this level is still largely adapted to the needs of recognition software. Level 3 incorporates both high resolution and multi-spectral image acquisition to permit a detailed morphological description of iris structure independent of any recognition algorithm.

Table 4-1. Suggested Feature Level Details for Iris

Classification	Fingerprint Meaning	Iris Equivalent
Level 1 features	Large scale patterns in the ridge flow of the print. Detection of core and delta regions and Henry-style classification. Require <500 DPI	Low frequency patterns in the overall composition of the iris as imaged in the near-infrared spectrum. Minimally adequate for repeatable automatic segmentation and algorithm matching. Require: 100 pixel iris diameter
Level 2 features	More granular features of ridge structure including bifurcations and terminations (i.e., minutiae) along with the presence of scars, creases, or incipient ridges. Require: 500 DPI	Intermediate iris structure sufficient to identify prominent instances of radial furrows, concentric furrows, pigment spots, crypts of Fuchs, and degenerations due to medical conditions or damage. Require: 200+ pixel iris diameter
Level 3 features	Detailed examination of ridge structure including the presence of pores and variations in shape or width. Require: 1000 DPI	Finely resolved iris features with spectral response characteristics (red, green, blue, infrared) necessary to identify both prominent and inconspicuous aspects of iris morphology and appearance. Require: 400+ pixel iris diameter at multiple wavelengths

To our knowledge, no definitions have yet been proposed for iris feature level details, but these should provide a good starting point for discussion and reference.

Assuming an average corneal diameter of 11.71 mm and a planar surface, the resolutions given above translate into the following pixel resolutions per millimeter.[5] This is in rough agreement with the ISO standard, which seems to presume a 12 mm diameter.

- 100 pixel diameter = 8.5 pixels/mm
- 150 pixel diameter = 12.8 pixels/mm
- 200 pixel diameter = 17.1 pixels/mm
- 400 pixel diameter = 34.2 pixels/mm

[5] Rufer F, Schroder A, Erb C. White-to-white corneal diameter: normal values in healthy humans obtained with the Orbscan II topography system. Cornea 2005;24(3):259-61.

Optical resolution measured in line pairs per millimeter depends on contrast assumptions. For illustration, the values above roughly correspond to the features discernable below.

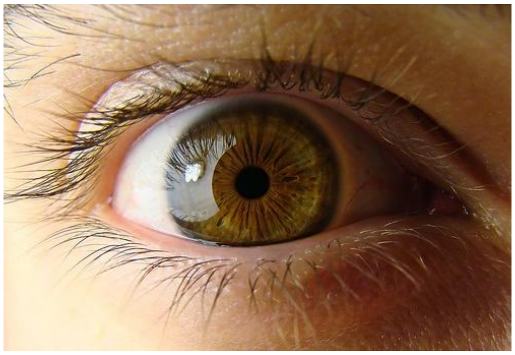

Figure 4-1a– Visible spectrum iris image

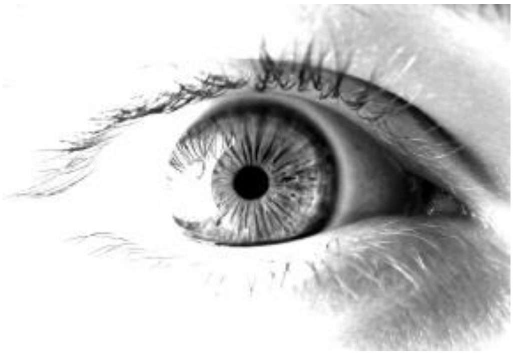

Figure 4-1b – Simulate Near Infrared image based[6]

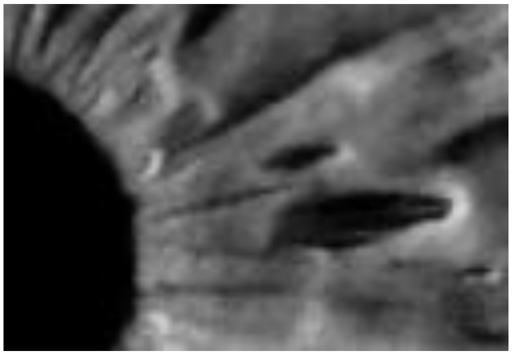

Figure 4-1c– 3x2mm iris section at 34.2 pixels/mm (400 pixel diameter)

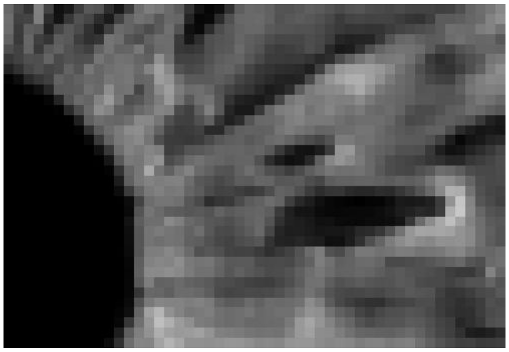

Figure 4-1d - 3x2mm iris section at 17.1 pixels/mm (200 pixel diameter)

[6] Eye image obtained from http://flickr.com/photos/no3rdw/2142399953/ publicly licensed by “no3rdw” (Paul <no last name> Troy, NY) on Dec. 27, 2007 under condition of attribution.

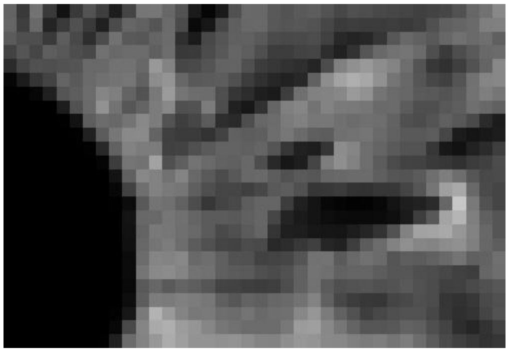

Figure 4-1e - 3x2mm iris section at 12.8 pixels/mm (150 pixel diameter)

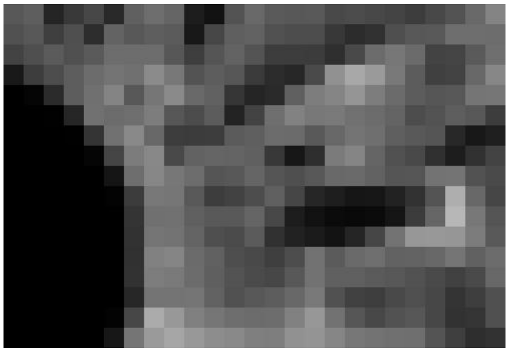

Figure 4-1f - 3x2mm iris section at 8.5 pixels/mm (100 pixel diameter)

Figure 4-1. Illustrations of Iris Features in Various Spectrums

The iris used above exhibited significant texture even in the visible spectrum. This is useful for illustration but is not typical of many eyes that require near-infrared illumination to reveal sufficient detail. The finer radial furrows are only visible at the highest resolution and quickly lose prominence even at 200 pixels. Eyes lacking in such rich detail may only resolve the largest furrows and crypts by the time the diameter is lowered to 100 pixels across the iris.

4.3 Testing and Evaluation

Several iris evaluations over the last few years may provide valuable insight into identifying certification criteria or areas needing further research.

IBG Independent Testing of Iris Recognition Technology (ITIRT) 2005

This report investigated operational performance between commercially available iris recognition devices. The data highlights the need for uniform quality metrics and imaging standards to achieve the greatest interoperability between systems. The report noted significant differences in performance when enrolling with one system and querying with another.

NIST Iris Challenge Evaluation 2006

ICE 2006 evaluated three recognition algorithms against data obtained at Notre Dame University. The data collection protocol bypassed some of the quality pre-filtering built into the sensor to help mitigate vendor bias. The results showed that there are minor accuracy differences between left and right eye performance, but these were statistically insignificant. Differences such as these suggest that human factors issues (e.g. placement, feedback,.) may need to be considered during criteria development, especially if dual-eye sensors are used.

<u>Authenti-Corp Iris Recognition Study 2006 (IRIS 2006)</u>

This study evaluated ISO/IEC 19794-6 compliant images collected from three commercially available recognition systems. It demonstrates that matching algorithms need to be adapted to different cameras to maintain accuracy.

<u>NIST Iris Exchange Evaluation 2008</u>

This evaluation is still in process but seeks to investigate iris format and interchange guidance as specified in ISO/IEC 19794-6:2005 and ANSI/NIST ITL 1-2007. It will specifically address a revised polar interchange format and various compressed formats.

4.4 Relevant Biometric Standards

Guidance on the acquisition, transfer, and storage of iris image data is provided by two primary standards. These documents share many attributes in common, reflecting joint development or close references.

- ANSI/NIST-ITL 1-2007: "American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information" (Annex I).
- ISO/IEC 19794-6-2005: "Information technology – Biometric data interchange formats – Iris image data."

ANSI/NIST-ITL 1-2007: "American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information" was approved in April 2007. Section 22 of the document provides packaging guidance for iris transmissions in the form of a Type-17 image.

The ISO ratified "ISO/IEC 19794-6: Information technology—Biometric data interchange formats—.Iris image data," in June 2005. The standard seeks to address four areas:

- Attributes necessary to exchange iris data within Common Biometric Exchange Formats Framework (CBEFF) biometric data blocks.
- Flexible image representations that maintain vendor interoperability under constrained bandwidth and storage situations.
- Limited image quality criteria necessary to ensure standards conformance.
- Iris presentation and acquisition recommendations.

4.5 Market Considerations

The commercial iris recognition market is almost completely descended from matching technologies developed by Iridian Inc. (now L-1 Identity Solutions). This technology was licensed to various device integrators who now share a de facto degree of interoperability.

4.6 Conclusion

Iris recognition systems have been simultaneously boosted and constrained by the dominance of a single vendor. The core technology, as licensed by Iridian (L-1 Identity Solutions) to several systems integrators, has created a de facto history of interoperability. Iris images and templates from one L1-licensed system are largely compatible with any other. Sensor interoperability tests in 2005 identified some shortcomings in the technology such as failures to enroll and accuracy loss across systems, but issues were not critical. Newer cameras can give higher resolution images, but the L1 algorithm is not configured to take advantage of it. The value of this higher resolution is currently unknown.

However, vendor and patent restrictions have prohibited a broader understanding of iris imaging and recognition by limiting more varied acquisition and interoperability testing. Iris templates are algorithm specific with little opportunity for a wider, interoperable definition across methods and vendors. The image capture process itself is subject to variations in illumination wavelength that are not well understood or measured. The NIST IREX 08 evaluation is aimed at establishing a standardized compact image format that approaches the size of a template and fills a template's roll.

Quality assessment has been closely coupled with sensor design and has made it nearly impossible to fairly assess algorithm performance using commercial imagers.

Iris sensors have enabled fairly high levels of performance despite using relatively low cost hardware that might not fare well using even moderate certification criteria. The Iridian algorithm relies on low frequency information and is tolerant of some blur. The needs of iris matching (for verification or identification) are fundamentally at odds with an analyst's need for identifiable features in a clear, high-contrast image.

4.7 Recommendations

- Baseline the current 'hidden' operational parameters [e.g. illumination wavelength, illumination geometry] currently used by commercial iris recognition systems and assess how susceptible the segmentation and recognition algorithms are to changes.
- Characterize commercial sensor quality in terms of MTF, SNR, wavelength, IR safety and other requirements. Harmonize sensor behavior with the needs of both human examiners and recognition software, and recommend minimal certification criteria.
- Socialize a common set of iris camera requirements between government agencies that are minimally necessary to enable enrollments, identifications, and verifications.
- Identify vendor neutral quality assessment tools to better understand what factors contribute to accurate identification and how to better provide feedback to operators.
- Begin identifying iris best-practices and environmental relationships to develop "Annex H/I" style acquisition guidance (See Appendix C for detail on ANSI/NIST-ITL 1-2007 Sections 15, Annex H and I).

- Identify iris features necessary to facilitate human identification tasks and map these back to objective resolution/quality metrics needed in the capture process.

5 General Certification Goals

5.1 Balancing Certification Goals

No single certification regimen may be appropriate for all use cases within a given biometric modality. In some cases, it may not even be justifiable to enumerate sensor certification criteria if the following conditions apply:

- At a reasonable price point, commercial sensor quality nominally exceeds any conventional requirement for biometric use in its intended environment.
- An existing corpus of technology evaluations, operational tests, or scenario experience indicates that current designs meet expectations.
- There is no identifiable need, partner agreement, or process in place for Level 3 details that would push sensor design to the next phase.
- Criteria linked to accuracy and interoperability are barely justified *and* in direct conflict with operational needs (e.g., ruggedness) as required by partners.
- The state of biometric matching software and its requirements for accuracy, do not justify the selection of the certification criteria, or either is irrelevant.

In cases where certification is difficult to justify, it may still be worthwhile to baseline current hardware designs to preserve known performance characteristics. Future developments may then be tested against this baseline to ensure that the changes represent real improvements without introducing subtle problems.

In cases where certification is desirable, the criteria may still vary based on the intended purpose. Fingerprint techniques have split to accommodate the needs of both verification (e.g., PIV – Personal Identity Verification) and identification (EBTS Appendix F). This will likely carry over to other biometric modalities and be amplified by the ability to sample subjects at a distance (e.g., facial surveillance), with minimal cooperation (e.g., Iris on the Move), or under severe portability restrictions (e.g., Hand-Held Interagency Identity Detection Equipment, or HIIDE).

As we move forward for other biometrics, stakeholders must be engaged early to help qualify existing and emerging use cases, operational limitations, and the effects on legacy data. Some of these considerations are listed below along with their implications. For some of these applications, aggressive certification may provide no real benefit since environmental or operational considerations dominate. Strict guidelines would only serve to increase costs and discourage partnerships. On the other hand, applications that explicitly (or automatically) enroll biometric data for subsequent analysis require stricter certification guidelines. The long term accuracy of the system and its suitability for future queries depends on avoiding quality degradation as databases grow.

Diverse Submitters – Local Law Enforcement

The diversity of training and resources will be a driving factor in the performance of many local law enforcement offices. Consistent imaging practices and environmental configuration will be more influential on accuracy than device performance. Cost pressures, lack of training and reliance on “value” devices suggests a larger need for process-based certification with continual monitoring of submissions for quality.

Intelligence Community Applications and Scenarios

Intelligence Community applications continually strive to reduce the operational constraints of biometric capture devices and minimize subject cooperation requirements. Biometric data is unlikely to exhibit predictable quality, and opportunity costs often prohibit the acquisition of additional images. Only the broadest certification guidelines necessary to ensure interoperability, but with no guarantees of accuracy, may be useful here.

Handheld Field Operations

Smaller field-grade systems are subject to tight considerations of weight, portability, power, ruggedness, and replaceability. Certification must recognize that environmental conditions will offset many of the stricter device attributes and negate those benefits. Even if the devices initially passed a strict regimen, calibration is difficult to maintain over the long term. Ease of use and consistency of operation should be mixed with broad considerations of interoperability. Overly strict quality guidelines are unlikely to be satisfied without conflicting with other goals.

Personal Verification

Verification tasks are subject to partitioning into both low and high security scenarios. Both require a high degree of automation with subject feedback, and certification guidelines should reflect these needs. Cost pressures for low-security applications can be mitigated by avoiding guidelines that are difficult to meet and provide only marginal accuracy improvements. Higher security applications can utilize a stricter certification process, and may include aspects of liveness detection and anti-spoofing measures.

Open Set Identification (watch list)

The accuracy of identification varies based on the size of the enrollment database and the number of biometric instances used for the match process. Strict certification is more desirable when using very large enrollment databases or when analyst review of match candidates is not possible. Policies that mandate auto-enrollment (i.e., retaining queries for later analysis and searching) require careful treatment of biometric data to avoid polluting the database with low quality samples.

Legacy Data Co-Mingling

All certification guidelines should consider the state of existing records and the effects on overall match performance and analyst review. Increases in image fidelity may introduce cross-channel inaccuracies as new data is compared with old data having different characteristics.

5.2 Certification as a Process

Ideally, certification is more of a process than merely a gatekeeper. The establishment of standards and criteria ensures that biometric designs meet or exceed the minimum attributes and behaviors needed to perform effectively. But once deployed in an operational setting, it is equally important to ensure that the biometric devices *continue* to function appropriately. This is decidedly more difficult and subject to many uncontrolled factors such as the environment, operator training, and subject variation.

Compliance Services

Continuous validation of device performance implies the need for a highly automated compliance service. This service should serve two functions and operate on imagery that is acquired and provided by external sources. The first is to provide a reference implementation for providing initial device assessment. Industry standard test targets, resolution charts, and procedures would support developers and testers who wish to submit new and revised designs for assessment. The service would provide a tentative pass/fail based on imagery captured remotely. A full assessment of new devices would naturally be performed under fully controlled conditions, but an automated service would offload many testing responsibilities and enhance the re-testing of established designs that have only undergone minor modifications or production changes.

The second function serves to provide continuous monitoring of operational data and ensure that quality is maintained over the biometric device lifetimes. This service runs in conjunction with normal submission workflow and monitors the quality of biometric imagery coming from diverse agencies, devices, and perhaps even operators. Instead of using test charts as in the previous case, this mode generates aggregate statistics from actual biometric imagery over time. This analysis enables the mitigation of several operationally relevant occurrences.

- Sensor quality at a particular installation degrades over time (due to age and wear) and would otherwise go unnoticed. Device(s) require replacement.
- Image quality originating from particular operators is sub-par due to a lack of training, operational pressures, or other human factors. Identify specific causes and mitigate at the source by instruction or reconfiguration.
- Systematic differences in quality from different agencies. Report on these differences to encourage (or enforce) improvements over time.

Certification-as a service requires open metrics for biometric quality assessment that go beyond metrics built into biometric devices. Baseline testing of device fundamentals can rely on ISO standard test practices and charts. These metrics are described in the standards literature and software is commercially available to automate the process. Despite the existence of these metrics, operational quality assessment of biometric imagery is still problematic.

For fingerprints, NIST has provided the NFIQ image analysis routines. These grade finger impressions into discrete quality bins. No such open tools currently exist for face or iris. For broad applicability and vendor independence, these tools need to be developed and tested using real, operational data. Ideally, the quality metrics should be returned as a continuous variable instead of a few discrete quality bins. Such measures facilitate the generation of aggregate statistics across many submissions. Vendor neutrality is necessary to avoid redundant assessments that only reaffirm built-in sensor decisions. Longer term, evolutionary developments also require a freely modifiable quality framework that matures over time as other expectations change.

6 Preliminary CPL Readiness Model(s)

There are several criteria that should be evaluated to determine when a biometric mode should be included in the CPL. Many of these criteria address specific technological issues necessary to ensure the maturity of the biometric. But they are also instrumental in determining the scientific lineage needed to establish Daubert criteria.

The criteria listed below are provided as guidance in the formation of a readiness model that seeks to objectively assess biometric readiness. They are only a subset of the possible factors that can be considered. No attempt has been made to emphasize the relative contribution of one entry over another.

6.1 FBI Interest

What is the demand for the biometric within a CJIS context?

- Does the biometric support current FBI identification needs?
- Can the biometric add value to an overall identity record?
- Will future partnerships or stakeholders influence the adoption of the biometric?

6.2 Research

How much research is available for the modality?

- How long has active research been ongoing?
- What is the reputation of the researchers and/or publications?
  Are the journals peer reviewed?
- What communities have been doing the investigation?

Are there any statistics on how unique the biometric is at a target resolution?

- Is the physiological or morphological basis of the biometric understood?
- Has investigation used diverse populations or narrow ones (e.g., students)?

- Are there data on the long and short term temporal stability of the biometric?

Is the trait genetically influenced? (twin problem)

6.3 Data (Testing and Evaluation Corpora)

Is there enough data to support the research and generate meaningful statistics?

- Do sensors produce raw images (or data) compliant with industry standards for vendor neutral matching and storage?
    - Has data been pre-filtered hand-manipulated for quality purposes?
- Can acquisition systems robustly produce data of consistent quality in the target environment?
- Are there sensor fidelity test methods and common calibration targets that are appropriate to the sensing of the target biometric? For example:
    - Non-optical sensing techniques such as capacitance based, ultra-sound, magnetic or acoustic
    - Non-contact optical sensors that are subject to variable distance, geometric distortion, motion, and ambient conditions (e.g. video sources)
    - Acoustics and voice
    - Biological samples.

6.4 Forensic Value

Is there an existing, mature capability for human forensic identification of samples of the new modality?

- Is it documented?
- Can samples be acquired without sensor-specific distortions of the underlying trait?

6.5 Interchange/File Format Standards

Are there any published standards for the modality so that the data can be exchanged with other agencies or one vendor's software switched out for another's?

- Qualify the maturity level
    - Image exchange only
    - Image capture and exchange with quality guidance
    - Interchangeable template representations
- Are standards operating at industry, national, or international scope?
- Do interchange standards exist in isolation or reference others?
    - Lower-level interchange formats, compressions.

  - o Device performance criteria.

6.6 Standard Operating Procedures (SOP)/Best Practices(BP)

Is there any SOP or BP for this modality?

- Are the operating procedures applicable to FBI needs (e.g. identification)?
- Have the procedures been subsequently assessed for performance/accuracy?

Are there open methods for assessing conformance with those practices, e.g. are there quality metrics for the biometric that are not vendor specific?

How does this modality change any SOP or BP that is already in use, e.g. can the new modality leverage existing guidance?

6.7 Market

Are there multiple vendors that make sensing devices for a given modality?

- Do patent or licensing restrictions limit competition?
- Do options exist if a critical vendor ceases operations?
- Is the technology primarily under foreign ownership?

Are there multiple vendors that make recognition algorithms for a given modality?

- Do patent or licensing restrictions limit competition?
- Do options exist if a critical vendor ceases operations?
- Is the technology primarily under foreign ownership?

Is the biometric marketplace maturing poorly in the absence of FBI involvement?

- Are other agencies and data collectors setting policy that will conflict with future FBI needs?
- Will data interoperability issues arise in the near future?
- Are ad hoc, compatibility choices being phased in out of necessity vs. planning?

7 Other Modalities—Potential and Constraints

In the long term, certification pressures have the potential to impact any biometric modality. As technologies mature and become broadly available, the focus will shift from basic performance to issues of interoperability and service-level compatibility. Premature certification efforts may impede biometric development; but conversely, delayed efforts risk needless incompatibilities and reduced accuracy as early systems become entrenched.

For illustration, we examine three additional biometric modalities that contrast with the issues described for face, iris, and fingerprint. Vascular recognition rounds out the imagery-based biometric methods, but this time with a dependence on internal physiological structures instead of externally visible ones. Voice exemplifies a mode with significant behavioral and environmental aspects that supersede anatomic considerations. Finally, DNA illustrates a physical sampling protocol with a substantial reliance on acquisition, storage, and handling procedures.

For additional background on these biometric modalities, refer to the Technology Assessment portion of this SABER document.

7.1 Vasculature (Vein Structures)

Vasculature recognition is the process of identifying individuals based on the structure of veins in the hand or capillaries in the finger. The technology is rooted in a medical understanding of how hemoglobin-rich blood absorbs near infrared illumination relative to surrounding tissue. These vascular structures form very early and, barring injury, stabilize at physical growth maturity.

Vascular recognition has only recently been commercialized (circa 2004) and has been marketed primarily in Asia by Hitachi and Fujitsu. Hitachi focuses on a finger sensor that matches capillary structures. Fujitsu uses a larger sensor that images the larger vein structures of the palm. A lesser known company, Techsphere (South Korea), markets a sensor that uses the back of the hand.

The acquisition of the vasculature structures is an active 2D imaging process. Near infrared light is used to illuminate the skin, tissues, and blood vessels. The different absorption characteristics cause the vasculature to stand out from the surrounding tissue which is then captured as an ordinary image. If the camera and illuminator are co-located, the technique is reflective and reveals surface structures. The palm and back-of-hand sensors use this method. If the camera and illuminator are placed opposite each other, the technique is transmissive and relies on light passing through the skin. This is suitable for smaller structures such as the finger and is employed by Hitachi.

In many respects, vasculature recognition is merely another imaging process and shares several of the certification issues discussed for face and iris sensors (e.g., wavelength, spatial resolution, noise, focus). But unlike those, vascular imaging is an internal physiological process with little intuitive basis for a human operator to ensure quality. Proprietary matching software further complicates this by concealing the underlying techniques and assumptions needed for processing. These imaging requirements may not even align with what a human examiner would ideally wish to see. Such sensor-to-algorithm bindings make it difficult to separate the imaging, quality analysis, and matching processes cleanly.

Nevertheless, we can identify several issues that would need to be investigated for a vascular certification regimen.

- What is the spatial resolution and grayscale depth necessary for raw imagery?
- Which compression formats and rates are best suited for imagery exchange?
- How large is the physical region that is to be imaged?
- How must the imagery be captured and/or represented (projection, normalizations, coordinate systems.)?
- What imaging wavelength (or combination) is best suited to a diverse population? Does it vary based on physiological, ethnic, or other factors?
- What are the ideal illumination energies and angles necessary to achieve sufficient tissue depth and vascular detail?
- Are there any eye-safety considerations (e.g., illuminator timeouts, intermittent pulses,.)?
- What liveness detection methods should be mandatory?
- What feedback mechanisms must be implemented to ensure that an operator can successfully assess proper image acquisition?

There is limited guidance from ISO/IEC 19794-9 (Information technology – Biometric data interchange formats – Part 9 – Vascular image data). This document provides an initial attempt at forging an interchange specification consistent with the usage of other 19794-class biometrics. However, the relative newness of the biometric and the limited number of vendors makes it difficult to proscribe much more than basic image-level storage.

7.2 Voice (Speaker Identification)

Speaker identification poses a serious challenge to certification because it is a behavioral biometric and subject to far greater environmental and subject variation. In other modalities, the physiological (i.e., anatomic) traits are sampled more directly and often in ways that can mitigate interference (e.g.. active illumination, narrow field of view, quality assessment, and retries). The properties that give the human voice uniqueness are rooted in the physiology of the mouth, throat, larynx, nasal cavity, and related regions. But the vibrations that constitute human speech are equally subject to many behavioral factors including:

- Rate and tone of speech (fast, slow, high, low)
- Language (dialect, non-native speakers, regional attributes)
- Style (read words, extemporaneous, formal, informal)
- Physical condition (health, age, tired).

Certification cannot address many of these issues other than acknowledging their contribution and trying to lessen their impacts by engineering a conducive baseline environment. For instance, a controlled enrollment scenario might favor consistency by using a comfortable room that encourages slow speech of a fixed body of text using well placed microphones.

From a sensor perspective, speaker identification is hampered by cross channel issues. These arise when voice samples are taken using one method (e.g., telephone) and compared against samples gathered in a different manner (e.g., desk microphone). Differences in sensors, room acoustics, and configuration decrease match accuracy. Many factors contribute to these differences, including:

- Room acoustics (reflection and absorption of sound)
- Distance of sensor to subject
- Signal to noise ratios and type of noise (e.g. white noise, roadway.)
- Sensor (microphone) characteristics (frequency response, vibration, directionality)
- Audio compression (lossy, lossless, cell phone, analog, digital)
- Integrated sensors (multi-microphone, noise cancellation).

The impact of these behavioral and environmental differences cannot be understated. Any certification plan must first identify the scenarios for which speaker identification is required. Once identified, the collection protocol and devices should be integrated to best suit the needs of that environment and ensure consistent acquisition. In this context, voice certification will likely bear a resemblance to facial acquisition. The device performance criteria are peered with the environmental configuration in which they must operate. These, in turn, must then be coupled with well-defined operator procedures necessary to ensure consistency and quality of the recordings.

ISO/IEC 19794-13 (Information technology – Biometric data interchange formats – Part 13 – Voice Data) is currently under development. It may be able to provide guidance on storage formats but is unlikely to substantially address speaker identification issues.

7.3 DNA

Unlike the biometrics treated previously, DNA processing requires a physically collected sample that must be gathered, prepared, stored, shipped, analyzed and reported according to well-defined procedures that ensure the quality and integrity of DNA processing, and protect the privacy of DNA processing results. These procedures are standardized by the FBI’s Scientific Working Group on DNA Analysis Methods (SWGDAM) and implemented through the FBI’s Combined DNA Index System (CODIS) program, which comprises systems at national, state, and local levels. These procedures and systems dictate FBI DNA processing capabilities and tools.

The FBI SWGDAM’s laboratory quality assurance procedures are documented in the Quality Assurance Standards for Forensic DNA Laboratories, October 1998, and the Quality Assurance Standards for DNA Databasing Laboratories, April 1999. Revisions to these two documents are effective July 2009. The SWGDAM established quality assurance audit procedures for all CODIS-participating laboratories in the FBI’s DNA Quality Assurance Standards Audit Document. The National DNA Index System (NDIS) Procedures Board implements policy regarding operations at the national level.

All laboratories participating in the CODIS program must be accredited, pursuant to the Justice for All Act of 2004. The American Society of Crime Laboratory Directors /Laboratory Accreditation Board (ASCLD/LAB), which is recognized as a CODIS-accrediting authority, provides a voluntary accreditation of member laboratories, both domestically and internationally, to ensure that member laboratories meet established standards and exhibit proper management practices. The ASCLD/LAB relies on ISO/IEC 17025:2005 (General requirements for the competence of testing and calibration laboratories) and SWGDAM standards, and performs external audits of labs for CODIS. The audit results are reviewed by the NDIS Audit Review Panel.

The American Board of Criminalistics (ABC) represents forensic scientists at the regional and national levels. They offer a certification in general criminalistics that includes trace evidence required for DNA analysis. The certification is voluntary and recognizes the professional knowledge, skills, and mechanisms needed to meet various disciplines. The ABC is itself, accredited by the Forensic Specialties Accreditation Board (FSAB).

Biometric data interchange standards are in development by ISO in line with other biometric modalities. The ISO/IEC [Working Draft] 19794-14: Biometric data interchange formats Part 14: DNA Data is in a preparatory stage having just undergone commentary. It extends the comprehensive 19794-x line of biometrics standards. A conformance testing methodology is also being developed under ISO/IEC 29109-14 and is also at a working draft stage.

Appendix A ISO Standards for Sensor Quality

Sensor Fidelity Metrics and Standards

The analysis of sensor fidelity has been treated in great detail by a series of ISO standards dating back nearly a decade. Their origins are rooted in the need to qualify the imaging behavior of any electronic still-picture device. Although not limited to biometric devices, they are applicable to any modality that relies on accurate imaging performance from typical "camera" devices.

Much of the processing required to conduct sensor testing has been automated by software packages in unison with applicable ISO test targets. Companies such as Imatest LLC[7] provide the tools, targets, and instructions necessary to automate evaluations. These tools are commonly used for professional digital camera reviews and should be transferable to a biometrics context should certification expectations change.

It may also be necessary to adopt a staged process of certification due to major differences in the digital camera vs. fingerprint markets. EFTS Appendix F established a precedent for fast-track certification when the vendor made minor modifications to a pre-certified device or added some value via limited integration. We must be willing to acknowledge that market factors (described later) in the digital camera market will exacerbate the need for rapid certification over a product's lifetime.

It may therefore be advantageous to classify capture requirements into three groups based on difficulty, stability, and dependence on environmental variations.

Class 1: Core design criteria fundamental to the device class

These criteria would be the most stringent and should be required for any new device being investigated. The act of certification would be to ascertain whether a new design or device class is fundamentally able to provide the quality and fidelity necessary to capture imagery successfully. These criteria would be roughly analogous to full certification in the fingerprint model.

Class 2: Manufacturing criteria that may vary based on production/acquisition cycles

These criteria would be used when there is reason to believe that a sensor model is undergoing subtle production changes or component substitutions. It is roughly equivalent to fast track certification and reflects the suspicion that device characteristics *may* have unintentionally been changed.

Class 3: Operational criteria subject to normal day-to-day conditions

These criteria represent tests that can be automated and fielded as software perhaps with the support of easy to use calibration targets. Because facial image acquisition will be subject to more environmental conditions than contact-based modes such as fingerprint, device issues should be

[7] Imatest LLC web site: http://www.imatest.com.

detected as early as possible. Tests in this class should be simple enough for any operator to perform in order to maintain proper device setup and usage.

The ISO has approved four photographic standards that characterize imaging sensor performance. Three pertain to electronic still-picture devices and one is targeted to photo scanners.

ISO 12233 – Electronic still-picture cameras – resolution measurements

This document identifies the characteristics necessary to resolve the finer details in a scene and addresses issues of the camera lens, photodetector, circuitry, and compressor. An image taken of a specially designed test chart and analyzed using a series of algorithms to determine the spatial frequency response of the equipment is shown in Figure A-1. The calibration chart supports four aspect rations from 1:1 (square) to 16:9 (widescreen).

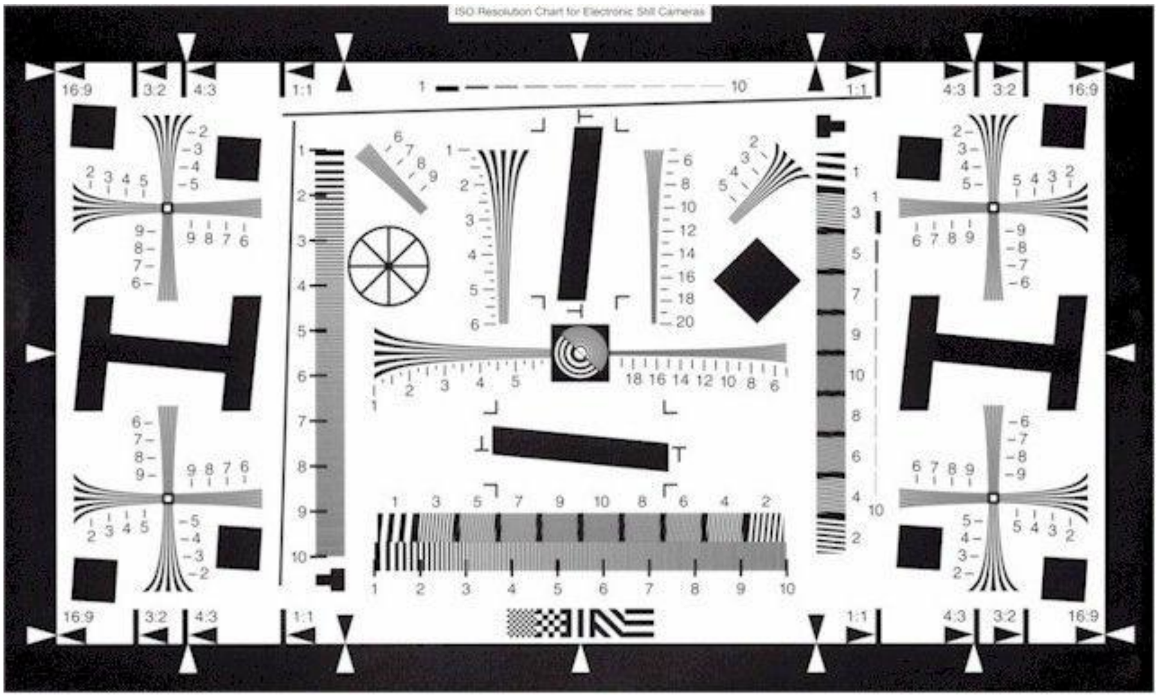

Figure A-1. ISO 12233 Calibration Chart

The standard includes a baseline algorithm for the calculation of various resolution measures including resolving power, limiting resolution, spatial frequency response, modulation transfer function, and optical transfer function. Although the test chart is designed for cameras with resolutions below 2,000 line widths per picture height, it can still be used by filling only a fraction of the sensor’s vertical range and extrapolating.

These metrics are crucial to understanding the ability of a camera to resolve the fine detail needed for level 3 facial features. It will be necessary to enumerate the classes and sizes of features that analysts look for and associate these with a resolution threshold that must be satisfied by a camera design.

ISO 14524 – Electronic still-picture cameras – Methods for measuring opto-electronic conversion functions (OECFs)

This document provides a methodology to characterize how the imaging device responds to a physical, optical input and reports it in a digital form. A test chart consisting of 12 stepped grayscale patches is imaged and analyzed to determine various imaging characteristics including white balancing, RGB agreement, contrast ratio, and dynamic range.

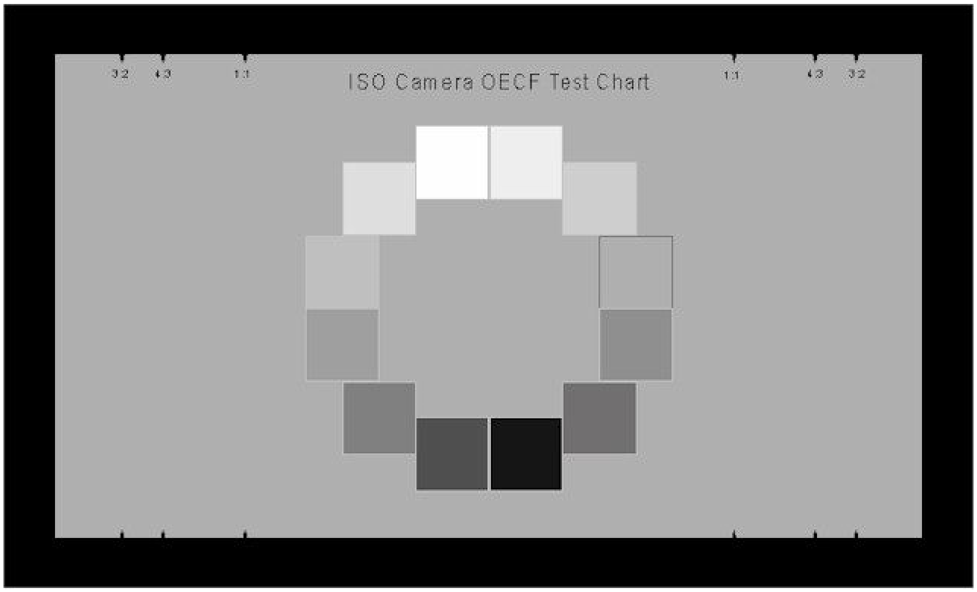

Figure A-2. ISA 14524 OECF Test Chart

Cameras exhibiting poor electro-optical conversion are more likely to yield overexposed imagery or poor color rendition, especially when the environment is less than ideal. Both of these conditions violate the expectations of ISO/IEC 19794-5 and may result in poor human recognition and/or algorithmic processing in grayscale space.

ISO 15739 – Electronic still-picture imaging – Noise measurements

This document specifies methods for characterizing imaging noise in the context of signal levels and dynamic range. It is applicable for both grayscale and color cameras. The perceived appearance of noise depends on many factors including its magnitude, its tonal context, and its spatial frequency. The visible appearance of the noise components will also vary for the luminance (grayscale) and color channels within an image. Exposure time, temperature, and gain controls will all affect the magnitude of noise within the image.

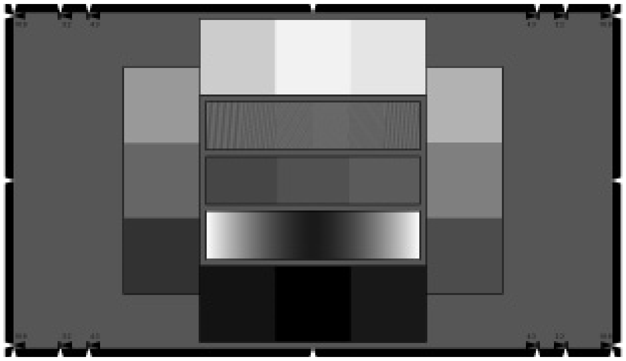

Figure A-3. ISO 15739 Test Chart

Camera designs may employ signal processing techniques to reduce noise during the acquisition process. These variables, and the interplay among them, need to be characterized in order to determine the ideal settings and thresholds for certification.

ISO 16067-1 – Spatial resolution measurements of electronic scanners for photographic images – Scanners for reflective media

This standard identifies the characteristics needed for a photograph scanner to capture fine details of the original photo. It is similar to both ISO 12233 and ISO 14524 and addresses spatial frequency response and opto-electronic conversion functions.

The stringency required for certification will depend on a characterization of typical mugshot photos that would be optically scanned. In the absence of a dominant print standard (c.f. fingerprint cards), low quality, legacy photos might not benefit from tight performance thresholds. Nevertheless, this standard provides a mechanism to align certification criteria between print and digital media types.

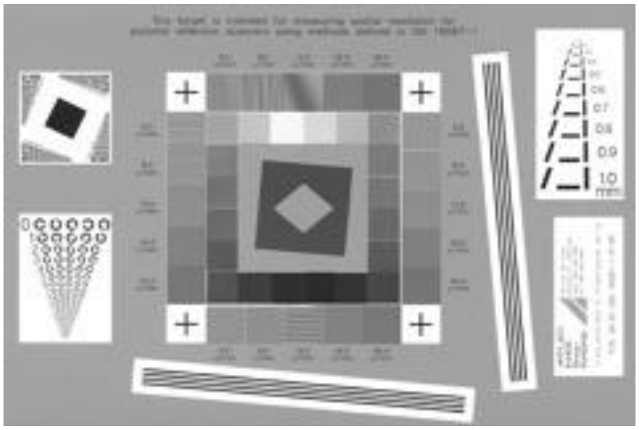
This target is intended for measuring spatial resolution for
pictorial reflection scanners using methods defined in ISO 16067-1
0.6
0.7
0.8
0.9
10
mm

Figure A-4. ISO 16067 Test Chart

Software can be purchased from vendors such as Imatest LLC to automate many of these calibration tests, including support of all the ISO test targets described above.

Appendix B ISO/IEC Iris Standards Provisions

After national standards are developed, they are often submitted for international approval. Many of the ANSI and INCITS documents were the precursors of the ISO/IEC standards described below. For biometrics, the job of standardization falls under sub-committee 37 (SC-37) of an ISO/IEC Joint Technical Committee (JTC1).

A detailed analysis of gaps and differences between the standards bodies is beyond the scope and intent of this document. However, the language and structure of the standards suggest that the ISO/IEC versions reflect most, if not all, of the biometric criteria contained in the earlier standards.

From an international partnership perspective, the use of ISO/IEC references may prove more useful than their ANSI/INCITS counterparts. In any case, normative references often point to ISO/IEC standards to qualify common image or video exchange formats (e.g., JPEG, MPEG).

ISO/IEC 19794-6 (Iris Image Data)

The ISO standard introduction notes that "compliance with this document may involve the use of patents concerning iris recognition given in Clause 6 and/or Annex A." Clause 6 provides the normative iris image format specification and Annex A gives the informative iris image capture criteria. The two sections, together, represent the bulk of the document.

ISO 19674-6 provides no guidance regarding human examination for verification purposes. Nor does it provide treatment of forensic needs or issues. The following table enumerates how the standard treats major requirements, how they relate to imaging fidelity, and any significant gaps.

Table B-1. ISO 19794-6 and Imaging Fidelity Links

Issue	ISO 19794-6 Guidance	Imaging Fidelity Linkage and Gaps
Color saturation	Color values over a 24-bit (RGB) image should permit grayscale conversion with at least 7-bit (128 values) fidelity.	See *Exposure*. What additional restrictions for grayscale conversion must be accommodated during camera testing?
Compression	Can be either RAW, JPEG, JPEG-Lossless or JPEG 2000. Compression ratio should be 6-to-1 or less.	Occluded regions that have been replaced with "fill values" (e.g. white and black) prohibit the use of compressed formats.

Issue	ISO 19794-6 Guidance	Imaging Fidelity Linkage and Gaps
Contrast	Image should have 70 grey levels between iris and sclera and 50 grey levels between pupil and iris.	Subject to amendment. May not always be possible for all ethnic groups
Focus	Merely states that images should be in focus and that Compression levels should preserve this.	Ties in with *Compression* level selection.
Grayscale density	The dynamic range over the image should be at least 7 bits (128 values) stored in at least 1 byte. Specularities should be set to the saturation value or black.	Implications of deriving grayscale intensity values from a color image are not addressed
Illumination	Suggests the use of near infrared illumination between 700 and 900 nm, but does not preclude other wavelengths. Illuminator should be 5 degrees alongside or below the camera to avoid red-eye and shadow.	Interoperability among recognition algorithms will vary based on differences in illumination wavelength.
Image scale	Presumes iris diameters between 9.5 and 13.7 mm. Image padding (matte) should be at least 70 pixels.	Image context (matting around the iris) doesn’t seem to depend on the resolution. Padding fulfillment should map to physical units, not pixels.
Noise	SNR should be less than 40 dB inclusive of compression noise.	No treatment of illumination intensity, aperture, or other imaging parameters that affect noise
Optical distortion	Should not exhibit spherical aberration, chromatic aberration, astigmatism, and coma.	Subjective [visual] treatment only
Pixel aspect	Calls for use of square pixels accurate within 1%.	Not clear if this must be a fundamental sensor trait or merely a system output (converted/adjusted).

Issue	**ISO 19794-6 Guidance**	**Imaging Fidelity Linkage and Gaps**
Preprocessing	Rectilinear and polar coordinate image storage is supported. The polar format permits the iris and pupil to have differing centers and non-concentric borders.	Preprocessing may be error prone and lead to some vendor-specific performance issues. Untested.
Quality	References four ranges mapped to the *Resolutions* but subject to focus, contrast, signal/noise ratio, and occlusion constraints.	No reference technique for assessing quality. Implementation is left up to the provider. Interpretation is left up to the receiver.
Resolution	Provides 4 categories (poor, low, medium, high) and the iris diameters (pixel resolutions) needed for fulfillment. The lowest category (poor) is deemed unacceptable for use.	The highest resolution (200 pixel iris diameter) is likely too low to supply Level 3 feature detail.
Visible Iris	70% of the iris should be visible and unobscured.	A behavioral issue and subject to amendment.

Appendix C   Face Recognition Guidance

ANSI/NIST-ITL 1-2007 Sections 15, Annex H and Annex I

Much of the standard addresses methods for best-practice image acquisition (e.g. lighting, positioning, framing.). Aspects of digital imaging performance are limited to quality stipulations that can be verified by simple operator inspection (e.g., good focus) or that directly map to aspects of image exchange (e.g., resolution). Nevertheless, the document provides a roadmap to understanding what is minimally necessary to ensure automated facial identification processes.

The ANSI/NIST-ITL 1-2007 standard seems to make the assumption that any reasonable quality digital camera can meet the formatting and image quality standards if it is used properly within the target environment. Despite the stated goal of enabling human examination for verification purposes, the document provides no treatment of forensic needs or issues. The following table enumerates how the standard treats major requirements, how they relate to imaging fidelity, and any significant gaps.

Table C-1. ANSI/NIST-ITL 1-2007 and Imaging Fidelity Links

Issue	ANSI/NIST-ITL 1-2007 Guidance	Imaging Fidelity Linkage and Gaps
Color Space	Device-independent color space, sRGB.	Sensor should provide a superset of capability with acknowledgement that final storage may change. An ideal sensor should have independent RGB sensors aligned in space (i.e., not Bayer filtered).
Exposure (over & under)	The expose shall be keyed to the background.	The camera must provide an effective range of luminance values (8-bit?) across the entire face. How should the camera determine exposure (globally or regionally)?
Focus and depth of field	The subject shall be in focus from nose to ears.	What will be the certified focal ratio (single or range) for camera testing? Should this be fixed or dynamically set by the camera?
Image compression	JPEG 2000 with broad treatment of compression rates.	Compression ratios, induced artifacts, and consistency issues (ROI compression) need to be addressed from a forensic perspective. Sensor accuracy must reflect pragmatic limitations imposed by later storage.

Issue	ANSI/NIST-ITL 1-2007 Guidance	Imaging Fidelity Linkage and Gaps
Interlacing	Video interlacing of odd and even scan lines is not permitted.	Not applicable to progressive digital camera designs, but image stabilization or other post-processing may need to be assessed and/or prohibited for compliance.
Radial distortion	Distortion should not be noticeable by human examination.	How strict should the tolerances be for certification testing? What should the optical settings be at the time of testing?
Red eye	Red eye is not allowed.	Illumination sources (flash, diffuse) are integral to camera design. How should these be addressed during certification?
Resolution	Varies based on Subject Acquisition Profile (SAP).	SAP's other than level 50 are probably insufficient for the resolution of finer, type 3 feature details.

The development of ANSI/NIST-ITL 1-2007 is based on the needs of facial recognition software in the 2003-2004 timeframe. The standard does not take a human-centric approach to the needs of facial verification, facial feature assessment, or attempt to identify the impact on level 2 & 3 feature classes. The introduction of variable, regional image compression (ROI) that treats the facial area differently from the rest of the subject and background may be troubling for forensic applications.

International standards

In December 2007, the ISO published ISO/IEC 19794-5:2007/Amd 1:2007 entitled *Conditions for taking photographs for face image data* as an amendment to the initial 19794-5 facial standard. It supplements Annex A (Best Practices for Face Images) of that document by providing expert guidance and best practices for the design of photographic studios and photo booths. It also addresses issues of printing quality and scanned face photographs for circumstances where digital image exchange is not possible. The amendment acts as Annex B to the original document.

The amendment describes the photographic environment necessary to achieve best practice image quality and provides specific configurations and recommendations. Topics include:

- Lighting arrangements when using a single light, dual lights, and dual lights with background lighting
- Positioning and distance recommendations between subject and camera
- Setups for photo studio and photo booth settings
- Printing quality guidelines
- Scanning quality guidelines
- Scene recommendations

- Photographic examples.

This document reflects some of the most operationally relevant guidance available for facial biometrics to date. It should serve as a capable starting point for developing best practice guidance for criminal justice imaging environments.

Appendix D Acronyms

ABC	American Board of Criminalistics
ANSI	American National Standards Institute
APB	Advisory Policy Board
ASCLD/LAB	American Society of Crime Laboratory Directors - Laboratory Accreditation Board
BOP	Bureau of Prisons
BP	Best Practices
CBEFF	Common Biometric Exchange Formats Framework
CFAIRS	Combined Face and Iris System
CJIS	Criminal Justice Information Services
CODIS	Combined DNA Index System
CPL	Certified Products List
DNA	Deoxyribonucleic Acid
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FSAB	Forensic Specialties Accreditation Board
HIIDE	Hand-held Interagency Identity Detection Equipment
IBG	International Biometric Group
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
IR	InfraRed
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
JPEG	Joint Photographic Expert Group

JTC1	Joint Technical Committee
LED	Light Emitting Diode
MPEG	Moving Picture Experts Group
MTF	Modulation Transfer Function
NDIS	National DNA Index System
NEC	Nippon Electric Company
NFIQ	NIST Fingerprint Image Quality
NGI	Next Generation Identification
NIST	National Institute of Standards and Technology
OECFs	Opto-Electronic Conversion Functions
PCR	Polymerase Chain Reaction
PIV	Personal Identity Verification
RGB	Red, Green, Blue
ROI	Regions of Interest
SABER	State of the Art Biometrics Excellence Roadmap
SAP	Subject Acquisition Profile
SNR	Signal to Noise Ratio
SOP	Standard Operating Procedures
STR	Short Tandem Repeat
UL	Underwriters Laboratory
USG	U.S. Government